

User Account Management

User Account Management involves several features such as password recovery, account recovery, user registration, locking user accounts and password policies, etc. In this tutorial, we are going to try functionalities related to identity management in WSO2 Identity Server.

WSO2 IS Configurations

Configure the email server

1. Configure the email server to send emails by following the below steps.
 - a. Open the `deployment.toml` file in the `<IS_HOME>/repository/conf` path.
 - b. Specify values for the `from_address`, `username`, and `password` parameters in the `[output_adapter.email]` section as shown in the extract below:

```
[output_adapter.email]
from_address="<email>"
username="<email>"
password="<password>"
hostname="smtp.gmail.com"
port=587
enable_start_tls=true
enable_authentication=true
```

(if you are using a gmail account as the sender, create an [App password](#))

and use that as the password. If your password contains invalid characters such as ">" , "<" and "&" , enter the password as "<![CDATA[xxxx]]>")

2. Navigate to `<IS_HOME>/bin` and start the server by executing either of the following commands.

Linux --> `sh wso2server.sh`

Windows --> `wso2server.bat`

3. Log in to the [Console App](#), and enter admin as both the username and the password.

Enable email invitations for user password setup

1. On the WSO2 Identity Server **Console menu bar**, click on the **Login & Registration** menu item.
2. When scrolled down a bit you will see the Invite User to Set Password option. Click on that.
3. From the given set of configuration check the box in front of **Enable email invitations for user password setup**.

Create a user

1. Expand the **User Management** menu item, click on **Users**.
2. On the **Users page**, click **Add User** and select **Single User** from the dropdown.
3. In the opened up wizard,
 - Keep **Primary** as the user store.
 - Add the below configuration to the respective fields.
 - Username: **tommy**
 - Email: **tommy@wso2.com**
 - First Name: **Tommy**
 - Last Name: **Dave**
4. Select **Invite the user to set their own password** option.
5. Select **Invite Via Email**.

Create User

Follow the steps to create a new user.

Basic Details User Groups

Enter the email address

First Name *

Enter the first name

Last Name *

Enter the last name

Select the method to set the user password

☒ Invite the user to set their own password

Invite Via Email Invite Offline

An email with a confirmation link will be sent to the provided email address for the user to set their own password.

☐ Set a password for the user

Cancel Save & Continue →

6. Click **Next**.
7. Skip group selection and Click **Save & Continue**.
8. The user will receive an email to **tommy@wso2.com** with an invitation link to set the password.
9. Open the **Invitation link** received.
10. Add a **password** and confirm it.
 - Ex: **Tommy@123**

Password Recovery

Introduction:

In this section we will configure Email based password recovery option.

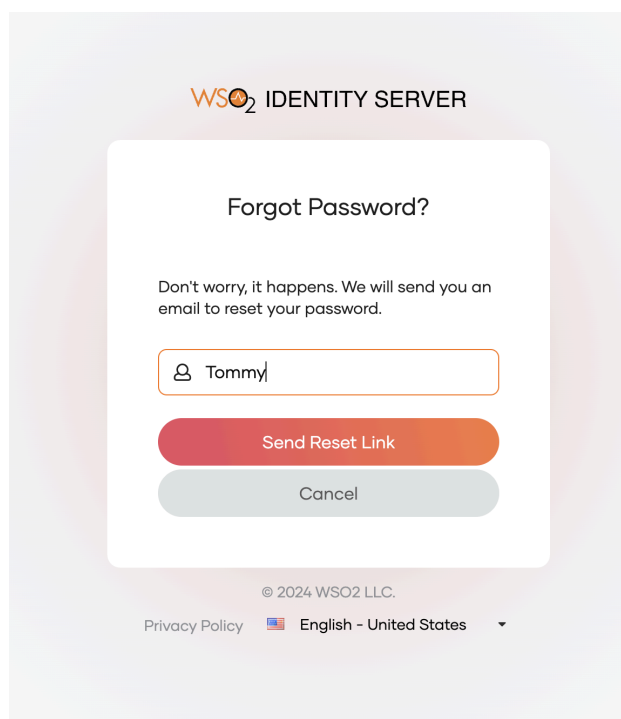
Setting up

1. In the WSO2 Identity Server **Console**, go to **Login & Registration > Account Recovery > Password Recovery**.
2. **Toggle** the switch to enable password recovery option to allow users to recover their passwords.
3. **Check Notify on successful recovery** to send a confirmation email upon successful password reset.
4. Click **Update** to save the changes.

The screenshot displays the WSO2 Identity Server Console interface. On the left is a navigation sidebar with options: Home, Applications, Connections, API Resources, Branding, User Management, User Attributes & Stores, Organizations, Login & Registration (highlighted), Email & SMS, Console Settings, and Server. The main content area is titled 'Password Recovery' and includes a 'Go back to login & registration' link. Below the title, it states: 'Enable self-service password recovery for users on the login page. The user will receive a password reset link via email upon request.' A toggle switch is set to 'Enabled'. A configuration box contains a checked checkbox for 'Notify on successful recovery' with a sub-note: 'This specifies whether to notify the user via an email when password recovery is successful.' Below this, the 'Recovery link expiry time' is set to '1440 mins' in a text input field. A sub-note states: 'Password recovery link expiry time in minutes.' At the bottom of the configuration box is an orange 'Update' button.

Try It

1. Go to [My Account](#).
2. Click the **Forgot Password**.
3. Enter the user's username.
4. Click **Send Reset Link**.



The screenshot shows the WSO2 Identity Server 'Forgot Password?' interface. At the top, the WSO2 logo and 'IDENTITY SERVER' are displayed. The main heading is 'Forgot Password?'. Below this, a message states: 'Don't worry, it happens. We will send you an email to reset your password.' There is a text input field with a user icon and the text 'Tommy'. Below the input field are two buttons: 'Send Reset Link' (orange) and 'Cancel' (gray). At the bottom, there is a copyright notice '© 2024 WSO2 LLC.', a 'Privacy Policy' link, and a language selector showing 'English - United States' with a dropdown arrow.

5. An email notification is sent to the user's email address. Click on the **Reset Password** button in the email.

Reset your password

Hi,

Please click the following button to securely reset the password of your account in the organization **carbon.super**:

[Reset Password](#)

WSO2 Identity Server

6. Enter a new password and click **Submit**.

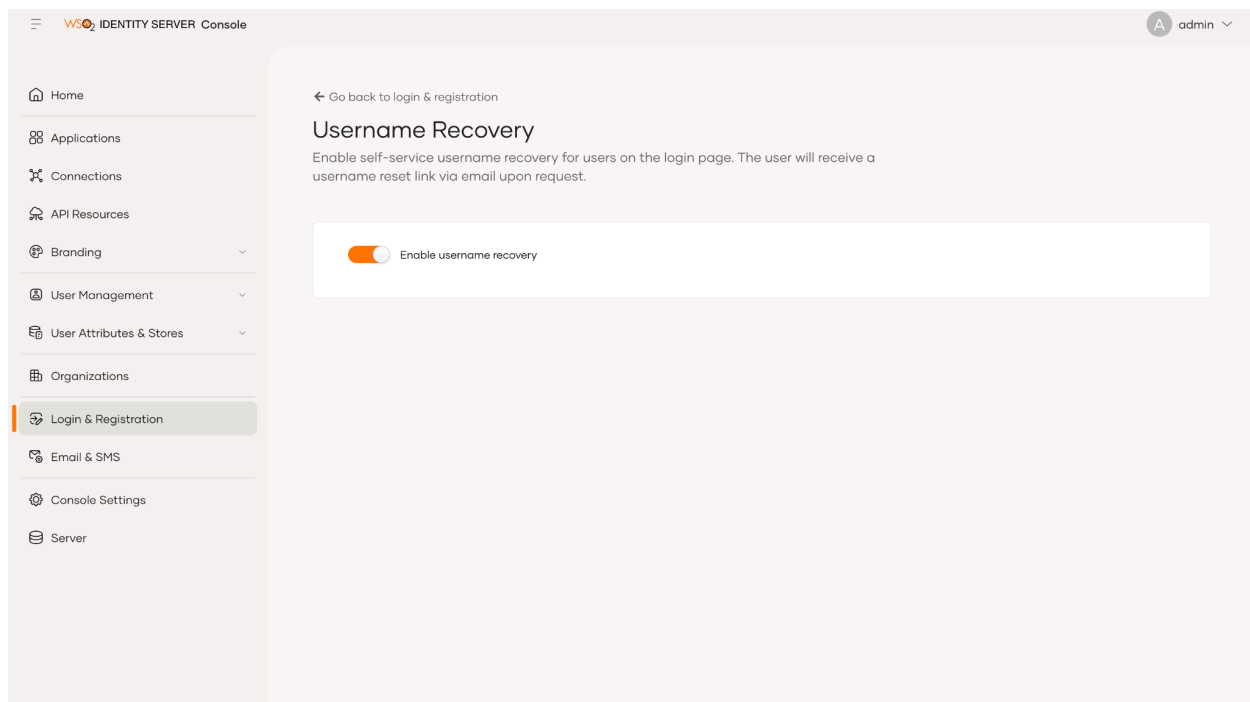
Username Recovery

Introduction:

In this section we will configure email based username recovery.

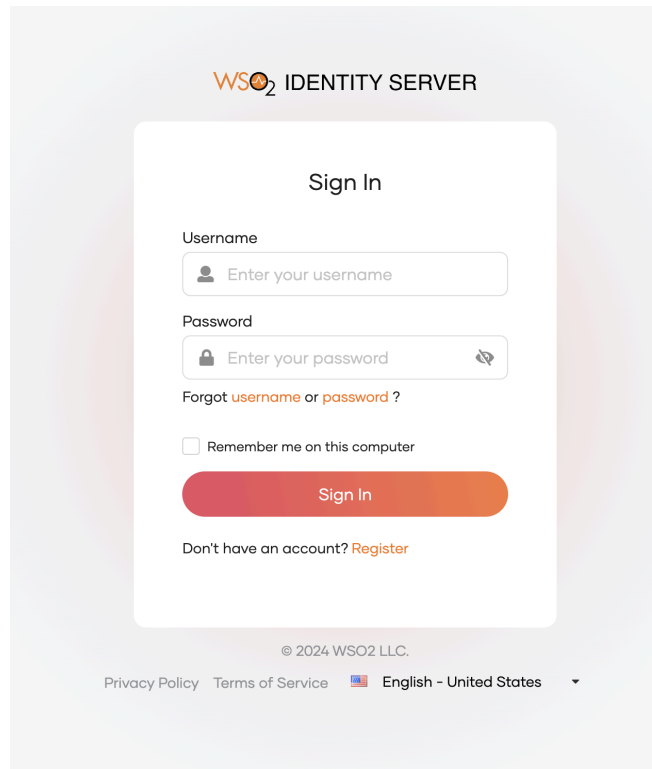
Setting up:

1. In the WSO2 Identity Server Console, go to **Login & Registration > Account Recovery > Username Recovery**.
2. **Toggle** the switch to enable the username recovery option to allow users to recover their passwords.

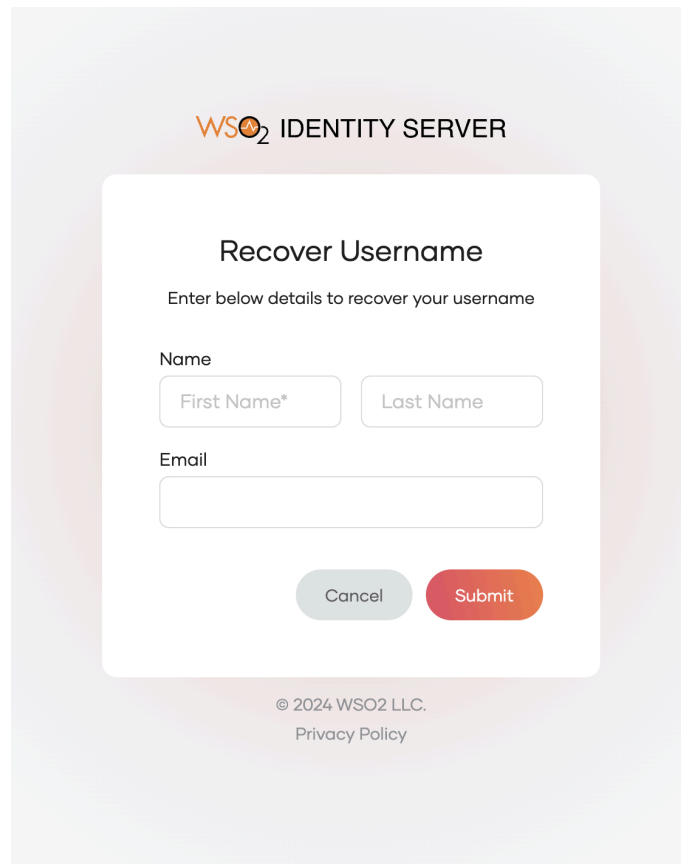


Try It:

1. Go to [My Account](#).
2. Click **Forgot username**.

The image shows a screenshot of the WSO2 Identity Server Sign In page. At the top, the WSO2 logo and the text "IDENTITY SERVER" are displayed. Below this, the heading "Sign In" is centered. The form contains two input fields: "Username" with a placeholder "Enter your username" and a user icon, and "Password" with a placeholder "Enter your password" and a lock icon. Below the password field is a link "Forgot username or password?". There is a checkbox labeled "Remember me on this computer". A large orange "Sign In" button is positioned below the checkbox. At the bottom of the form, there is a link "Don't have an account? Register". The footer of the page includes the copyright notice "© 2024 WSO2 LLC.", links for "Privacy Policy" and "Terms of Service", and a language selector showing "English - United States" with a dropdown arrow.

3. Enter all the required fields and click **Submit**.



WSO₂ IDENTITY SERVER

Recover Username

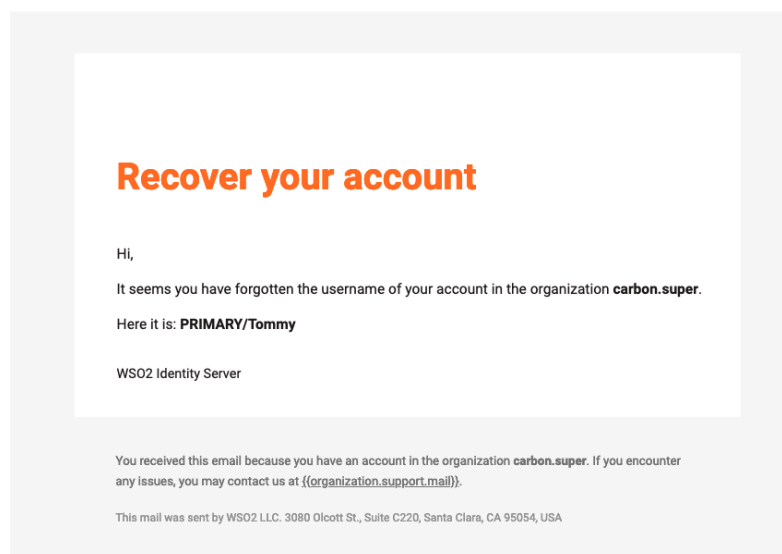
Enter below details to recover your username

Name

Email

© 2024 WSO2 LLC.
[Privacy Policy](#)

4. An email notification will be sent to the user's email address with the recovered username.



Recover your account

Hi,

It seems you have forgotten the username of your account in the organization **carbon.super**.

Here it is: **PRIMARY/Tommy**

WSO2 Identity Server

You received this email because you have an account in the organization **carbon.super**. If you encounter any issues, you may contact us at [{{organization.support.mail}}](#).

This mail was sent by WSO2 LLC. 3080 Olcott St., Suite C220, Santa Clara, CA 95054, USA

Account Locking

Introduction

The account locking feature is used to temporarily block a user from logging in. Account locking can be done by an administrative user or it can be configured to automatically lock upon multiple failed login attempts.

Setting up:

1. To show more specific error messages on the login page, the following property can be configured in the `deployment.toml` file in

`<IS_HOME>/repository/conf` path.

```
[authentication.authenticator.basic.parameters]
showAuthFailureReason=true
showAuthFailureReasonOnLoginPage=true
```

2. **Restart** the server.

Account Locking by an administrator

Setting up:

1. On the WSO2 Identity Server **Console**, expand the **User Management** menu item, click on **Users**.
2. Select the user **Tommy**.

The screenshot displays the WSO2 Identity Server Console interface. On the left, a sidebar menu lists various management options, with 'User Management' expanded and 'Users' selected. The main content area shows the profile of a user named 'Tommy'. The profile includes fields for User ID, Username, First Name, Last Name, Country, Email, and Mobile. The 'Lock user' option is visible at the bottom of the page.

WSO2 IDENTITY SERVER Console

admin

Go back to Users

Tommy
Tommy Kate

Profile Groups Roles Active Sessions

User ID
faa0584d-dc44-44af-a490-96ffca0355d

Username
Tommy

First Name *
Tommy

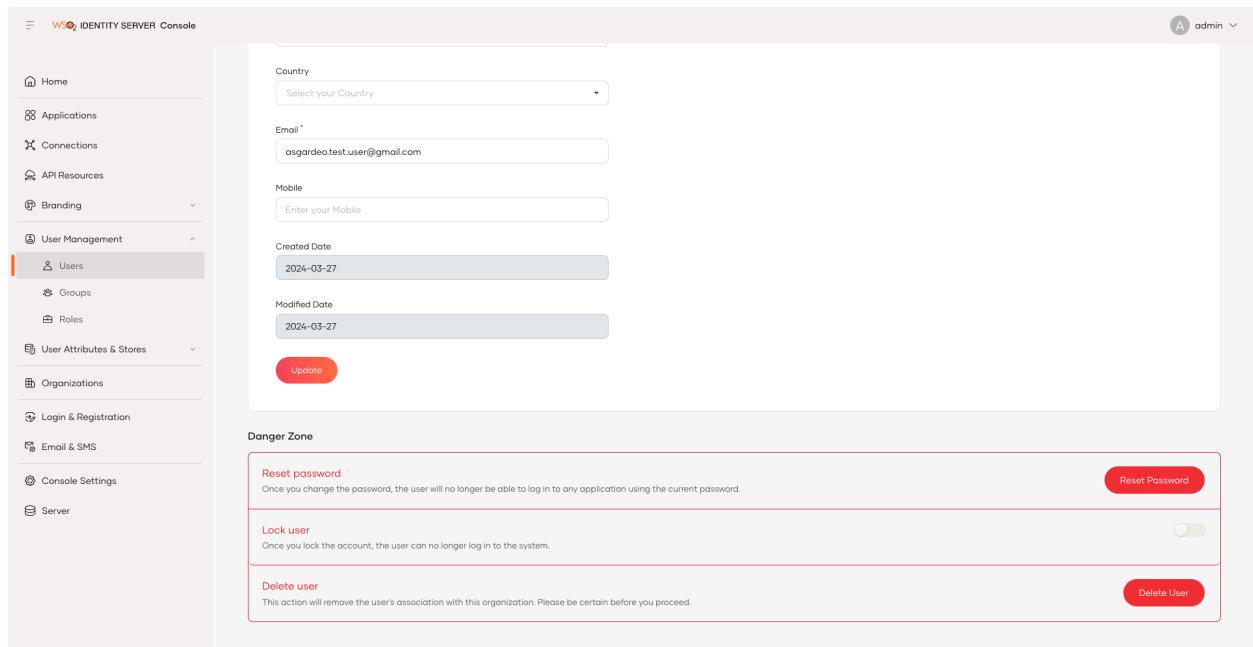
Last Name *
Kate

Country
Select your Country

Email *
asgardeo.test.user@gmail.com

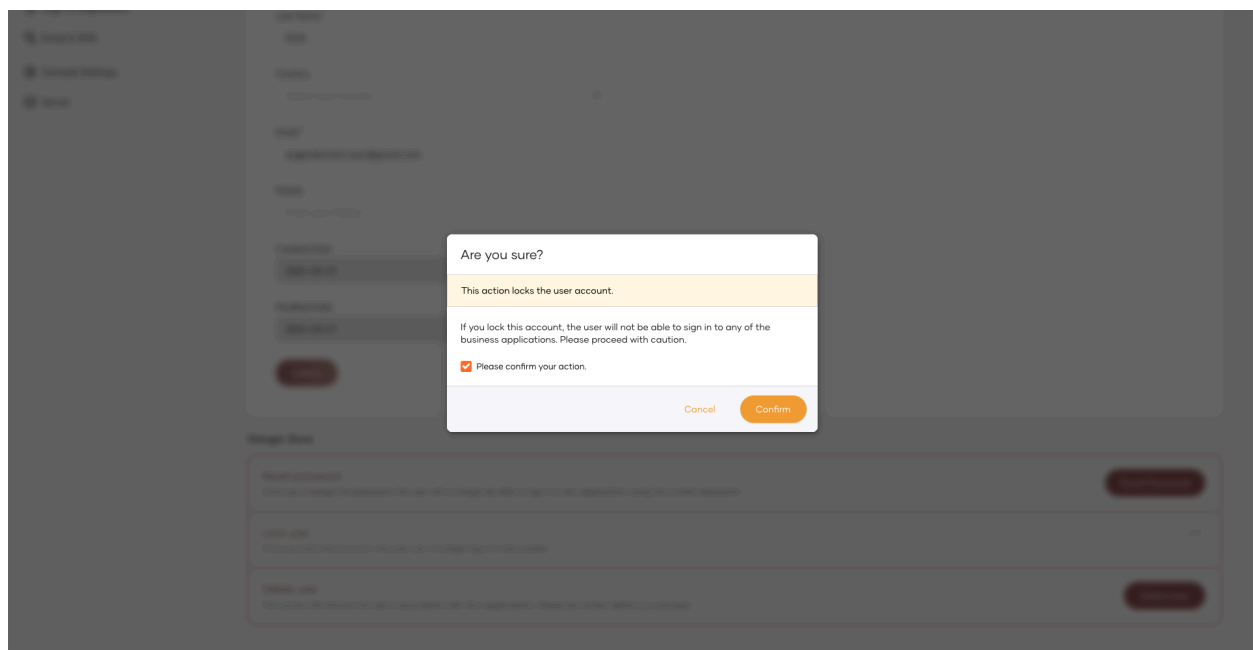
Mobile
Enter your Mobile

3. Toggle the button on **Lock user** option at the bottom of the page.



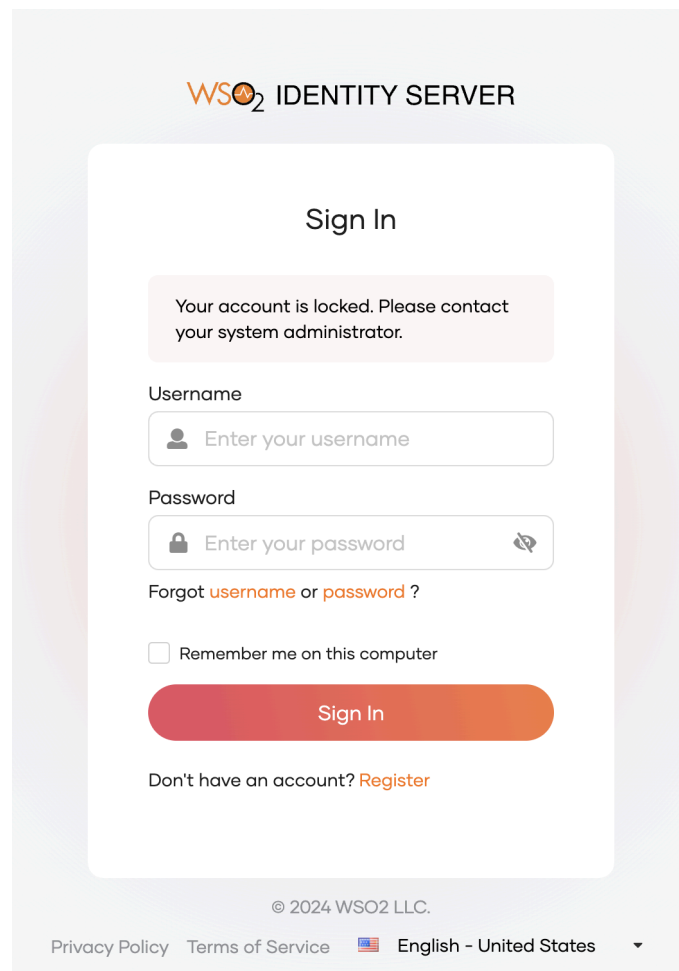
The screenshot shows the WSO2 Identity Server Console interface. On the left is a sidebar menu with options: Home, Applications, Connections, API Resources, Branding, User Management (expanded), Groups, Roles, User Attributes & Stores, Organizations, Login & Registration, Email & SMS, Console Settings, and Server. The 'Users' option under 'User Management' is selected. The main content area displays a user profile for 'asgardeo.test.user@gmail.com'. Fields include Country (a dropdown menu), Email, Mobile (a text input), Created Date (2024-03-27), and Modified Date (2024-03-27). Below these fields is an 'Update' button. At the bottom, there is a 'Danger Zone' section with three actions: 'Reset password' (with a 'Reset Password' button), 'Lock user' (with a toggle switch), and 'Delete user' (with a 'Delete User' button). Each action includes a warning message about the consequences of the action.

4. Check the **Please confirm your action** check box in the pop up.



Try It:

1. Go to [My Account](#), and try to login as the user you locked.
2. Now the login attempt will fail.



The image shows a screenshot of the WSO2 Identity Server Sign In page. At the top, the WSO2 logo and 'IDENTITY SERVER' text are displayed. Below this, the 'Sign In' heading is centered. A light pink message box states: 'Your account is locked. Please contact your system administrator.' Below the message, there are input fields for 'Username' and 'Password'. The 'Username' field has a placeholder 'Enter your username' and a user icon. The 'Password' field has a placeholder 'Enter your password', a lock icon, and a toggle icon. Below the password field, there is a link 'Forgot username or password?'. A checkbox labeled 'Remember me on this computer' is present. A large orange 'Sign In' button is at the bottom of the form. Below the button, there is a link 'Don't have an account? Register'. At the very bottom, the footer contains '© 2024 WSO2 LLC.', 'Privacy Policy', 'Terms of Service', a US flag icon, 'English - United States', and a dropdown arrow.

3. An email notification will be sent to the user's email address mentioning the account has been locked.

Account Locking based on failed login attempts

Setting up:

1. In the WSO2 Identity Server Console, go to **Login & Registration > Login Security > Login Attempts**
2. **Toggle** the switch to enable lock user accounts on failed attempts.

WSO2 IDENTITY SERVER Console

admin

Home

Applications

Connections

API Resources

Branding

User Management

Users

Groups

Roles

User Attributes & Stores

Organizations

Login & Registration

Email & SMS

Console Settings

Server

Go back to login & registration

Login Attempts

Protect user accounts from password brute-force attacks by locking the account on consecutive failed login attempts.

☒ Enabled

Once the account is locked, the account owner will be informed via email. The account will be automatically activated after the account lock duration.

Number of consecutive failed login attempts *

5

This specifies the number of consecutive failed login attempts allowed before the account is locked.

Account lock duration *

5 mins

This specifies the initial duration that the account will be locked for. The account will be automatically unlocked after this time period.

Account lock duration increment factor

2

This specifies the factor by which the account lock duration should be incremented on further failed login attempts after the account is locked.

How it works

Note: The following example is based on the above configurations.

User tries to login with an incorrect password in 5 consecutive attempts. User account will be locked for 5 minutes.

After 5 minutes

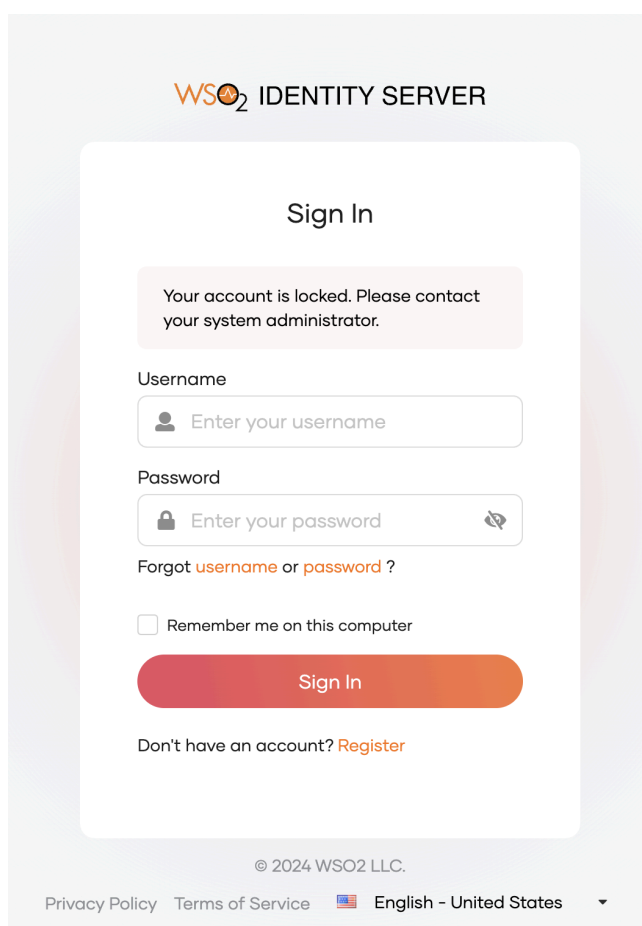
3. Specify Maximum failed login attempts as follows.

Maximum failed login attempts: 3

4. Click **Update**.

Try It:

1. Go to [My Account](#), and try to login giving wrong passwords 3 times.
2. Now try to login using actual credentials. Now your login attempt will fail as the account got locked.
3. An email that informs about the account locking is sent to the given email address.



The image shows the WSO2 Identity Server Sign In page. At the top, the WSO2 logo and 'IDENTITY SERVER' are displayed. Below this is a 'Sign In' heading. A pink message box states: 'Your account is locked. Please contact your system administrator.' Below the message are input fields for 'Username' and 'Password'. The 'Username' field has a placeholder 'Enter your username' and a user icon. The 'Password' field has a placeholder 'Enter your password', a lock icon, and an eye icon for toggling visibility. Below the password field is a link: 'Forgot [username](#) or [password](#) ?'. There is a checkbox labeled 'Remember me on this computer'. A large orange 'Sign In' button is below the checkbox. At the bottom, there is a link: 'Don't have an account? [Register](#)'. The footer contains copyright information '© 2024 WSO2 LLC.', links for 'Privacy Policy' and 'Terms of Service', and a language selector showing 'English - United States' with a dropdown arrow.

4. Wait for 5 minutes and try to log in again with the correct credentials. The WSO2 Identity Server Dashboard home screen appears.

Password Policies

Password Policies are some set of rules that enhance the users to use strong passwords. WSO2 Identity server helps you to customize password patterns so as to enforce stronger password policies.

Password Input Validation

Introduction

Password input validation involves checking the validity of passwords entered by users against certain criteria or rules in real-time. Using this feature, organizations can enforce the users to input passwords that meet the required length, complexity, and other specified criteria for passwords.

Setting up:

1. In the WSO2 Identity Server Console, go to **Login & Registration > Login Security > Password Validation**.
2. Adjust password policies accordingly. Change the following fields.

Password Input Validation

- Must be between 5 and 10 characters
- Must contain at least 2 numbers (0-9).

WSO₂ IDENTITY SERVER Console

admin

Home

Applications

Connections

API Resources

Branding

User Management

User Attributes & Stores

Organizations

Login & Registration

Email & SMS

Console Settings

Server

Go back to login & registration

Password Validation

Customize password validation rules for your users.

Password Expiration

☐ Password expires in 30 days

Password History Count

☐ Must be different from the last 5 passwords.

Specify the number of unique passwords that a user should use before an old password can be reused.

Password Input Validation

Must be between 8 and 30 characters

Must contain at least

1 numbers (0-9)

1 upper-case characters (A-Z)

1 lower-case characters (a-z)

1 special characters (!@#\$%^&*).

☐ Must contain at least 1 unique characters.

☐ Must not contain more than 1 repeated characters.

3. Click **Update**.

Try It:

1. Access the WSO2 Identity Server dashboard using the following link: [My Account](#)
2. Click **Forgot Password**.
3. Enter the user's username.
4. Click **Send Reset Link**.
5. An email notification is sent to the user's email address. Click on the **Reset Password** button given on the email.
6. Enter a password which violates the password patterns specified. It will give the error specified. Ex: Tom@1234567

WSO₂ IDENTITY SERVER

Reset Password

Enter new password

Tom@1234567



- ✗ Must be between 5 and 10 characters
- ✓ At least 1 uppercase and 1 lowercase character(s)
- ✓ At least 2 number(s)
- ✓ At least 1 special character(s)

Confirm password



☐ Both passwords should match

Proceed

© 2024 WSO2 LLC.

[Privacy Policy](#)



English - United States



Password History

Introduction

This feature helps to prevent users from configuring passwords that were used in the recent past. For example, if you configure a count of 2 passwords, users will be prevented from reusing their last 2 passwords as the current password.

Setting up:

1. In the WSO2 Identity Server Console, go to **Login & Registration > Login Security > Password Validation**.
2. Under the **Password History Count** check the checkbox for the option that says **Must be different from last __ passwords**.
3. Add 1 as the number of passwords.

The screenshot shows the WSO2 Identity Server Console interface. On the left is a sidebar with navigation links: Home, Applications, Connections, API Resources, Branding, User Management, User Attributes & Stores, Organizations, Login & Registration (highlighted), Email & SMS, Console Settings, and Server. The main content area is titled 'Password Validation' with a subtitle 'Customize password validation rules for your users.' Below this, there are three sections: 'Password Expiration' with a checkbox for 'Password expires in 30 days'; 'Password History Count' with a checked checkbox 'Must be different from the last 5 passwords' (highlighted with a red box) and a blue tip box stating 'Specify the number of unique passwords that a user should use before an old password can be reused.'; and 'Password Input Validation' with settings for length (8 to 30 characters) and character requirements (1 number, 1 upper-case, 1 lower-case, 1 special character, 1 unique character, and 1 non-repeating character).

4. Click **Update**.

Try It:

1. Access the WSO2 Identity Server dashboard using the following link: [My Account](#)
2. Click **Forgot Password**.
3. Enter the user's username.
4. Click **Send Reset Link**.
5. An email notification is sent to the user's email address. Click on the **Reset Password** button given on the email.
6. Enter the existing password. It will give the error specified. Ex: **Tom@1234**

WSO₂ IDENTITY SERVER

Reset Password

This password has been used in recent history. Please choose a different password.

Enter new password

☐ Must be between 5 and 10 characters
☐ At least 1 uppercase and 1 lowercase character(s)
☐ At least 2 number(s)
☐ At least 1 special character(s)

Confirm password

☐ Both passwords should match

Proceed

© 2024 WSO2 LLC.
[Privacy Policy](#)